中小企業の情報セキュリティ対策ガイドライン

第3版

IPA 独立行政法人情報処理推進機構
セキュリティセンター

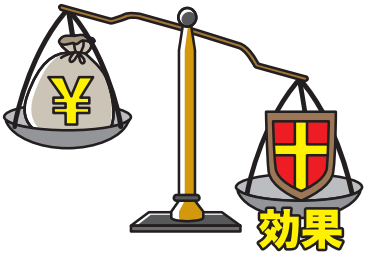
目　次

はじめに

1 経営者の皆様へ

本ガイドラインは、中小企業の皆様に情報を安全に管理することの重要性についてご認識いただき、中小企業にとって重要な情報[1]を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介することを目的としたものです。

情報セキュリティ対策は、経営に大きな影響を与えます！



情報セキュリティ対策を実施して対外的にアピールすることで、企業としての信頼性を確保し売上を伸ばしている企業がある一方、情報セキュリティ対策を疎かにしたために秘密情報や個人情報の漏えいを発生させ、業績は落ち込み、経営を揺るがしかねない高額な賠償金を支払った企業もあります。(➡ 詳細はP6)

対策の不備により経営者が法的・道義的責任を問われます！

現代社会では金銭や物品だけでなく、情報にも価値や権利が認められます。例えば個人情報保護法では、事業者に対して個人の権利利益の保護、安全管理措置などの管理監督が義務付けられており、これらへの違反が認められると場合によっては会社に罰金刑が課されます。さらに、取締役や監査役は、別途、会社法上の忠実義務違反の責任を問われることもあります。(➡ 詳細はP8)

組織として対策するために、担当者への指示が必要です！

企業の継続的な発展のために、また、経営責任を果たすためには、担当者に任せきりにすることなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくことが必要です。情報セキュリティ対策は、経営者が主導し、必要な範囲を網羅し、関係者と連携して組織的に実施しなければ機能しません。経営者はこれらを認識したうえで、情報セキュリティ対策の取り組みを担当者に指示する必要があります。(➡ 詳細はP10)

1 ▲**重要な情報**　営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報のことです。経済的価値を指す“資産”を加え“情報資産”と呼ばれることがあり、本ガイドラインでも“重要情報”に加え“情報資産”と表記します。

2 本ガイドラインの対象

本ガイドラインは、業種を問わず中小企業および小規模事業者（法人、個人事業主、各種団体も含む）を対象として、その経営者と情報管理を統括する方を想定読者としています。

3 本ガイドラインの全体構成

本編２部と付録により構成されます（表１）。付録には、情報セキュリティ対策の実施に活用できるサンプルが含まれています。

【表1】本ガイドラインの全体構成

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

第３版の主な変更点について

■第１部

- ITにあまり詳しくない経営者の方々にも理解していただけるよう、専門用語などをなるべく排して説明するように見直しました。
- 重要７項目の取組について、「サイバーセキュリティ経営ガイドライン」の改定に伴い、内容を一部更新することで整合性を維持しました。

■第２部

- 組織的な対策実施体制を段階的に進めていけるよう、全体構成を見直しました。
- 「セキュリティポリシー」については多様な解釈があるため、位置づけが明確になるよう、「基本方針」と「関連規程」に分けました。
- 「ウェブサイトの情報セキュリティ」、「クラウドサービスの情報セキュリティ」に関する解説を追加しました。
- 「SECURITY ACTION 自己宣言制度」との関連を意図したコラムを追加しました。

■付録

- 「中小企業のためのクラウドサービス安全利用の手引き」（付録６）を加えました。
- 旧版で付録「情報セキュリティポリシーサンプル」の一部であった「情報セキュリティ基本方針」を抜き出し、「情報セキュリティ基本方針（サンプル）」（付録２）としました。また、残り部分の名称を「情報セキュリティ関連規程」（付録５）に変更しています。

4 本ガイドラインの活用方法

本ガイドラインの活用にあたって、情報セキュリティに組織的に取り組んだ経験は必要ありません。本ガイドラインにより、事業の特徴に応じた情報セキュリティ対策を段階的に進めていくことができます。「**第１部 経営編**」は、全ての経営者に読んでいただきたい内容です。まずはご一読ください。「**第２部 実践編**」は、あなたの組織にあったSTEPから進めてください。

取組状況とアクション	本ガイドラインの活用方法
Step1 **まず始めましょう**	これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.17) を参照して、「情報セキュリティ５か条」を実行してください。 **進め方** 「情報セキュリティ５か条」を社内で配付するなど、まずできるところから開始してください。
Step2 **現状を知り改善しましょう**	Step1 は実施できていて次に進める場合は **「3. 組織的な取り組みを開始する」**（P.18）を参照して、「５分でできる！情報セキュリティ自社診断」で自社の状況を把握し、できていない対策の実行に努めてください。 **進め方** ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。 ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。
Step3 **本格的に取り組みましょう**	Step2 までは実施できていて次に進める場合は **「4. 本格的に取り組む」**（P.22）を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。 **進め方** ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。
Step4 **改善を続けましょう**	**「5. より強固にするための方策」**（P.30）を参照して、自社に必要な対策を追加実施してください。Step 1 や Step 2 に取り組んでいる企業でも、Step 4 を参照して必要な対策があれば実行してください。

第１部　経営者編

経営者編では、情報セキュリティ対策に関して、
経営者が認識し、
自らの責任で考えなければならない
事項について説明します。

1 情報セキュリティ対策を怠ることで企業が被る不利益

ITの普及や利活用により経営効率が向上した反面、ITの普及以前には想定し得なかった秘密情報や個人情報の漏えいによる、高額の賠償請求や金銭的損失を伴う事故が増えています。さらに、近年では事故やその影響も多様化し、金銭的損失以外の不利益も顕著になっています。こうした事故による不利益は、情報セキュリティ対策を行うことで、経営上受容できる範囲まで減らすことができます。

ここでは、情報セキュリティ対策の必要性に対する理解を深めていただくために、対策が不十分なために起きる事故と、それにより企業が被る主な不利益を次に挙げる4点に要約して説明します。

(企業が被る主な不利益)

●金銭の損失　●顧客の喪失　●業務の停滞　●従業員への影響

これらを参考に、自社で起きかねない情報セキュリティ上の事故とは何か、どの業務にそのような心配があるか、自社の経営において最も懸念される事態は何かなどを具体的に思い描くことが、経営者が情報セキュリティ対策を認識する第一歩です。このような思考実験が経営者によるリスク認識の基礎となります。

(1) 金銭の損失

取引先などから預かった機密情報や個人情報を万一漏えいさせてしまった場合は、取引先や顧客などから損害賠償請求を受けるなど、大きな経済的損失を受けることになります。

一方、こうした損害賠償などによる損失だけでなく、インターネットバンキングに関連した不正送金やクレジットカードの不正利用などで直接的な損失を被る企業の数も増えています。

事例1　ウイルス感染で数日間業務が停止し、数千万円の被害が発生

(所在地：東京都／業種：情報通信業／従業員規模：101～300名)

社内のパソコンやサーバーがウイルスに感染し、数日間に亘った業務停止に至る障害が発生した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。その後、ウイルス対策ソフトや技術的な対策の導入、情報セキュリティ規則の制定、プライバシーマークやISMS認証取得に取り組み、再発防止に努めている。

(2) 顧客の喪失

重要な情報に関する事故を発生させると、その原因が何であれ、事故を起こした企業に対する管理責任が問われ、社会的評価は低下します。同じ製品やサービスを提供している企業が他にあれば、事故を起こしていない企業の製品やサービスを選択する顧客が増えるのは自然なことであり、事故の発覚直後には大きなダメージを受けることになります。

大手メーカーのサプライチェーンに位置する企業の場合は、これまで継続してきた受注が停止に追い込まれることにもなりかねません。事故を起こした企業は再発防止に努め、事故を起こさずに事業を続けていくことが必要ですが、低下した社会的信用の回復には時間を要するため、事業の存続が困難になる場合もあります。

事例2　顧客情報の入ったパソコンの紛失事故により取引先の信用を失墜

(所在地：東京都／業種：情報通信業／従業員規模：101 ～ 300 名)

従業員が顧客情報の入ったパソコンを持ち出した時に紛失事故が発生した。顧客に対して紛失の報告をしたが信用を失うこととなった。原因は、会社として情報セキュリティに対する意識が高くなかったため、持ち出しに関する明確なルールや手続きを定めておらず、従業員がパソコンを自由に持ち出せる環境であったことである。その後、情報機器の暗号化などの対策を実施するとともに、パソコンの持ち出しルールを含めた情報セキュリティ規程を整備して従業員へ情報セキュリティ教育を行った。

(3) 業務の停滞

日常業務で使用している業務システムに事故が発生すると、原因調査や被害の拡大防止のために、運用中の情報システムを停止したり、インターネット接続を遮断しなければならないことがあります。その結果、電子メールが使えなくなるなど、業務が停滞し、納期遅れや営業機会の損失が生じるなど、事業全体に影響が出てしまいます。

事例3　ウイルス感染により基幹システムが一週間停止

(所在地：静岡県／業種：製造業／従業員規模：51 ～ 100 名)

従業員がメールに添付されていたウイルス付きのファイルを不用意に開いたことで感染し、基幹システムで障害が発生した。システムベンダーの協力を得て障害対応を行ったが、復旧するまでの一週間、基幹システムが使用できなくなった。原因は不審メールを受信した際の対処方法を詳しく教育していなかったことである。その後、朝礼などを利用して従業員へ情報セキュリティ教育を行うとともに、迷惑メール除去ツールを導入した。

(4) 従業員への影響

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、従業員のモラル低下を招く要因となります。さらに事故を起こしたにも関わらず、従業員のみを罰して管理職が責任を取らないような対応は、従業員が働く意欲を失うおそれがあります。情報漏えいなどの事故による企業としてのイメージダウンを嫌って、転職する従業員も現れます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。ある経営者は「個別の損害より、職場環境が暗くなったことが一番困った」と語っています。

2 経営者が負う責任

情報セキュリティ対策を的確に指揮しなかったことに起因する業績の悪化などが経営者の責任であることは言うまでもありませんが、それ以外の経営者の「法的責任」と「社会的責任」について説明します。

(1) 経営者などに問われる法的責任

企業が個人情報などの法的な管理義務がある情報を適切に管理していなかった場合、経営者や役員、担当者は表2に示すような刑事罰その他の責任を問われることになります。

- 個人情報やマイナンバーに関する違反の場合は刑事罰が科されるおそれがあります。また、個人情報保護委員会[2]による立入検査を受ける責任もあります。
- 民法上の不法行為とみなされた場合は、経営者が個人として損害賠償責任を負う場合もあります。

【表2】情報管理が不適切な場合の処罰など

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	40条 報告及び立入検査 83条 個人情報データベース等不正提供罪[3] 84条 委員会からの命令に違反 85条 委員会への虚偽の報告など 87条 両罰規定	委員会による立入検査、帳簿書類等の物件検査及び質問 1年以下の懲役又は50万円以下の罰金 6月以下の懲役又は30万円以下の罰金 30万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
マイナンバー法（番号法） 行政手続における特定の個人を識別するための番号の利用等に関する法律	48条 正当な理由なく特定個人情報ファイルを提供 49条 不正な利益を図る目的で、個人番号を提供又は盗用 50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用 51条 人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得 53条 委員会からの命令に違反 54条 委員会への虚偽の報告など 55条 偽りその他不正の手段により個人番号カード等を取得 57条 両罰規定	4年以下の懲役若しくは200万円以下の罰金又は併科 3年以下の懲役若しくは150万円以下の罰金又は併科 同上 3年以下の懲役又は150万円以下の罰金 2年以下の懲役又は50万円以下の罰金 1年以下の懲役又は50万円以下の罰金 6月以下の懲役又は50万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	3条 差止請求 4条 損害賠償請求 14条 信頼回復措置請求	利益を侵害された者からの侵害の停止又は予防の請求 利益を侵害した者は損害を賠償する責任 信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	197条の2 刑事罰 207条1項2号 両罰規定 198条の2 没収・追徴 175条 課徴金	5年以下の懲役若しくは500万円以下の罰金又はこれらの併科 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑 犯罪行為により得た財産の必要的没収・追徴 違反者の経済的利得相当額
民法	709条 不法行為による損害賠償	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う

2 **▲個人情報保護委員会**　個人情報保護委員会は公正取引委員会と同様の高い独立性を有する機関です。

3 **▲データベース等不正提供罪**　改正個人情報保護法で新設され、役員・従業者等が不正な利益を図る目的で個人情報データベース等を他者に提供等したり盗用した場合は処罰対象になります。

(2) 関係者や社会に対する責任

適切に管理することを前提に預かった情報を漏えいしてしまった場合に問われるのは、前述の法的責任に加え、その情報の提供者や顧客などの関係者に対する責任もあります。また、情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらしますので、会社役員が会社法上の責任(会社に対する損害賠償責任)を問われ株主代表訴訟を提起されることもあり得ます。さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまいます。したがって、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要です。

コラム

個人情報保護法

個人情報保護法は、企業や団体に個人情報をきちんと大切に取り扱ったうえで、有効に活用できるよう共通のルールを定めた法律です[4]。「氏名」、「生年月日」、「住所・電話番号・メールアドレス」などの連絡先、「顔写真」など、事業によって取り扱う個人情報は様々です。従業員情報や取引先の名刺も個人情報に当たりますので、従業員名簿やメールのアドレス帳などを作成している事業者は、保有する個人情報が少なくても、個人情報取扱事業者(個人情報データベース等を事業の用に供している者)となり、この法律が適用されます。

個人情報保護法について詳しく知るには個人情報保護委員会のウェブサイトを確認してください。

●個人情報保護委員会のウェブサイト
https://www.ppc.go.jp/

不正競争防止法

企業が持つ営業情報や技術情報などの中には、秘密とすることで差別化や競争力の源泉となる情報もあります。そのような情報が漏えいすると、研究開発投資の回収機会を失ったり、社会的な信用の低下により顧客を失ったりと大きな損失を被ることになります。秘密としている情報を不正競争防止法により営業秘密として法的保護を受けるためには、次の①～③の要件をすべて満たす必要があります。

①秘密として管理されていること(秘密管理性)
②生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であること(有用性)
③公然と知られていないこと(非公知性)

4 ▲個人情報保護法第1条には「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」とあることから、個人情報保護とは企業が被る損害の防止だけではなく、個人の人格的、財産的な権利利益に対する侵害防止を目的としていることに留意する必要があります。

3 経営者は何をやらなければならないのか

企業で情報セキュリティを確保するための、経営者の役割を説明します。情報セキュリティの確保に向けて、経営者は、(1)に示す「3原則」について認識したうえで、(2)に示す「重要7項目の取組」の実施を指示する必要があります。

(1)認識すべき「3原則」

経営者は、以下の3原則を認識し、対策を進める必要があります。

原則1　情報セキュリティ対策は経営者のリーダーシップで進める

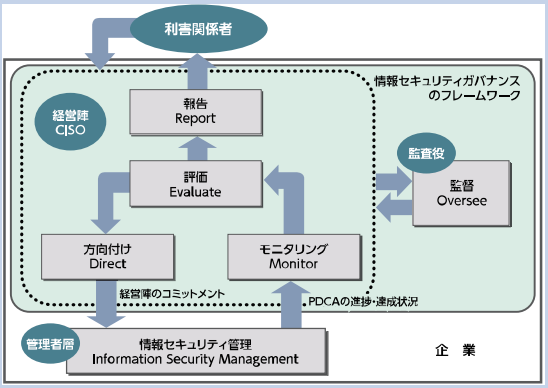
経営者は、IT活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策を進めます。現場の従業員は、安心して業務に従事できる環境を求める一方、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そこで、情報セキュリティ対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策の実施を主導します。

コラム

情報セキュリティガバナンス

情報セキュリティガバナンスは、経営者が企業戦略として情報セキュリティ向上に取り組むための枠組みです。

この枠組みは、経営者が懸念する避けるべき重大事故などを示して「方向付け」を行い、対策の進捗や点検等により状況を「モニタリング」し、その効果を「評価」して方向付けを見直すサイクルを骨格としています。

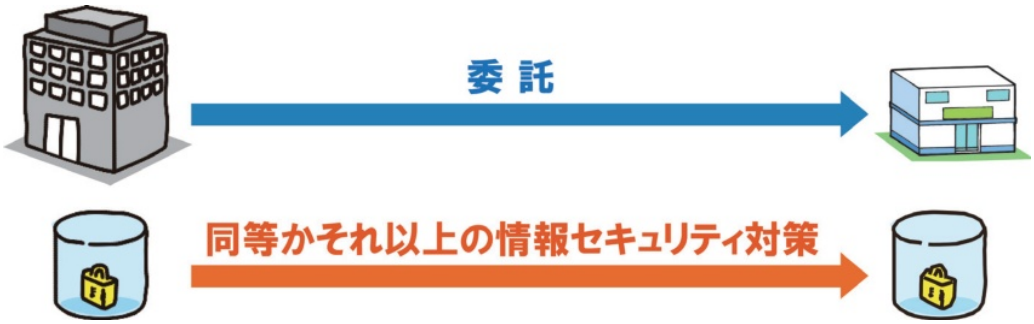


経営者がリーダーシップを発揮する枠組みでもあります。

●経済産業省『情報セキュリティガバナンスの概念』
http://www.meti.go.jp/policy/netsecurity/secgov-concept.html

原則 2　委託先の情報セキュリティ対策まで考慮する

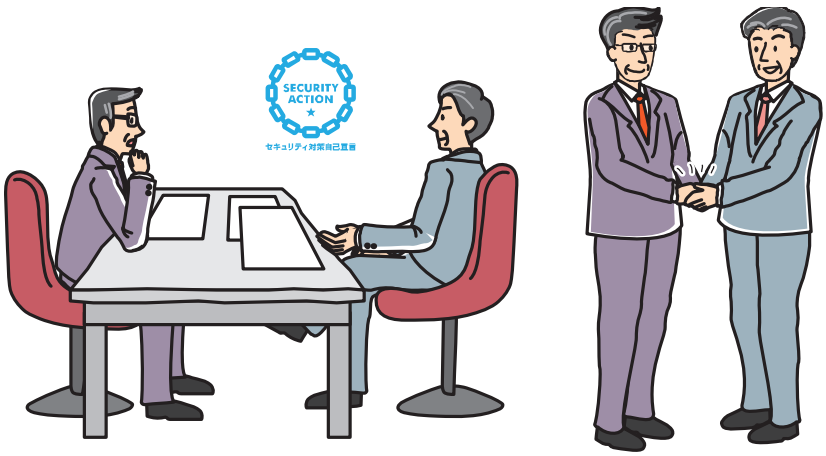
業務の一部を外部に委託するにあたって重要な情報を委託先に提供する場合、委託先がどのような情報セキュリティ対策を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんされたとき、それが委託先の不備だったとしても、事故の影響を受ける者から委託元としての管理責任を問われることになります。そのため、委託先や、共同で仕事を行っているビジネスパートナーなどの情報セキュリティ対策に関しても、自社同様に十分な注意を払います。また、受託している場合には、委託元の要求に応じる必要があります。



原則 3　関係者とは常に情報セキュリティに関するコミュニケーションをとる

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からの信頼を高めるには、普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。

情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、必要以上の不安を与えることなく、信頼関係を維持することができます。



(2) 実行すべき「重要7項目の取組」

中小企業で情報セキュリティを確保するための、経営者の役割を説明します。経営者は、以下の重要7項目の取組について、自ら実践するか、実際に情報セキュリティ対策を実践するうえでの責任者・担当者に対して指示します。場合によっては、経営者自らが実行することも必要になると考えられます。

取組 1　情報セキュリティに関する組織全体の対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した情報セキュリティに関する基本方針を定め、宣言します。自社の経営において最も懸念される事態は何かを明確にすることで具体的な対策を促し、組織としての方針を立てやすくなります。

取組 2　情報セキュリティ対策のための予算や人材などを確保する

情報セキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます。情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービス[5]の利用も検討します。

取組 3　必要と考えられる対策を検討させて実行を指示する

懸念される事態に関連する情報や業務を整理し、損害を受ける可能性(リスク)を把握したうえで、責任者・担当者に対策を検討させます。必要とされる対策には予算を与え、実行を指示します。実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示します。

実行を指示した情報セキュリティ対策がどのように現場で実施されているかにつき、月次や四半期ごとなど適切な機会をとらえて報告させ、進捗や効果を把握します。

取組 4　情報セキュリティ対策に関する適宜の見直しを指示する

取組3で指示した情報セキュリティ対策について、実施状況を点検させ、取組1で定めた方針に沿って進んでいるかどうかの評価をします。また業務や顧客の期待の変化なども踏まえて基本方針なども適宜見直しを行い、致命的な被害につながらないよう、対策の追加や改善などを行うように、責任者・担当者に指示します。

5 ▲専門的な外部サービスについてはIPAが公開している「情報セキュリティサービス基準適合サービスリスト」を活用することができます。(P.39 コラム「情報セキュリティサービス基準審査登録制度」参照)

取組 5　緊急時の対応や復旧のための体制を整備する

万が一に備えて、緊急時の対応体制を整備します。被害原因を速やかに追究して被害の拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的です。経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。

取組 6　委託や外部サービス利用の際にはセキュリティに関する責任を明確にする

業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書に情報セキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。

IT システム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、外部サービスを利用したほうが、コスト面から有利な場合がありますが、安易に利用することなく、利用規約や付随する情報セキュリティ対策などを十分に検討するよう担当者に指示する必要があります。

取組 7　情報セキュリティに関する最新動向を収集する

情報技術の進化の早さから、実施を検討するべき対策は目まぐるしく変化します。自社だけで把握することは困難なため、情報セキュリティに関する最新動向を発信している公的機関[6]などを把握しておき、常時参照することで備えるように情報セキュリティ担当者に指示します。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

6▲情報セキュリティに関する最新動向を発信している公的機関
IPA（独立行政法人情報処理推進機構）のウェブサイト　https://www.ipa.go.jp/security/index.html
NISC（内閣サイバーセキュリティセンター）のウェブサイト　https://www.nisc.go.jp/

コラム

「SECURITY ACTION」一つ星を宣言しよう！

「SECURITY ACTION（セキュリティアクション）」は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。取り組み段階に応じて、「一つ星」「二つ星」のロゴマークを無料で使用することができます。

「一つ星」は、情報セキュリティ５か条に取り組むことを宣言するものです。

情報セキュリティ５か条

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

これらの項目は、企業の規模に関わらず、必ず実行すべき重要な対策です。第２部に進む前に経営者のトップダウンで実行を開始して、自社が情報セキュリティ対策の取り組みを開始したことを自己宣言しましょう。

宣言方法や制度詳細は公式サイトをご確認ください。

●SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/

第２部　実践編

実践編では、情報セキュリティ対策を実践する
責任者・担当者を対象に、
実務的な進め方について説明します。

1 実践編の進め方

ここでは、経営者の指示に従い、どのように情報セキュリティ対策を実践していくかについて説明します。情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。

しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

そこで、本ガイドラインでは、規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐにできることから開始して、段階的にステップアップすることで、企業それぞれの事情に適した対策が実施できるように進め方を説明するとともに、実践のために各種の付録を用意しました。第1部で説明した重要7項目の取り組みとの対応を示した表3を参考に、自社の状況にあった進め方をしてください。

【表3】重要7項目の取り組みと実践編の対応表

実践編		ページ	取組1	取組2	取組3	取組4	取組5	取組6	取組7
2	できるところから始める								
	(1) 情報セキュリティ5か条	17			●				●
3	組織的な取り組みを開始する								
	(1) 情報セキュリティ基本方針の作成と周知	18	●						
	(2) 実施状況の把握	18			●				
	(3) 対策の決定と周知	20			●				
4	本格的に取り組む								
	(1) 管理体制の構築	22		●					
	(2) IT利活用方針と情報セキュリティの予算化	23					●		
	(3) 情報セキュリティ規程の作成	24		●					
	(4) 委託時の対策	26			●				
	(5) 点検と改善	28						●	
5	より強固にするための方策								
	(1) 情報収集と共有	31				●			
	(2) ウェブサイトの情報セキュリティ	32							●
	(3) クラウドサービスの情報セキュリティ	34				●			
	(4) 情報セキュリティサービスの活用	38				●			
	(5) 技術的対策例と活用	40				●			
	(6) 詳細リスク分析の実施方法	44				●			

2 できるところから始める

(1)情報セキュリティ５か条

多くの中小企業にとっては、いきなり精巧な対策を開始するのは大変なことだと思います。**「情報セキュリティ５か条」(付録１)**では、企業の規模に関わらず、必ず実行すべき重要な対策を５か条にまとめています。

インターネットの普及に伴い様々な脅威が現れ、攻撃者の手口は年々巧妙かつ悪質になっていますが、対策には共通する部分があります。情報セキュリティ５か条は、共通的な基本的対策をまとめたものですので、必ず実行しましょう。

① OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

② ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

③ パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

④ 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

⑤ 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

3 組織的な取り組みを開始する

(1) 情報セキュリティ基本方針の作成と周知

経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために、簡潔な文書を作ります。基本方針には、決まった書き方はありませんので、**「情報セキュリティ基本方針(サンプル)」(付録2)**を参考にして、事業の特徴や顧客の期待などを考慮したうえで経営者と連携しつつ、自社に適した基本方針を作成してください。

また、基本方針は従業員の指針であり、関係者に対して取り組みを表明するためのものなので、作成した文書は、従業員や顧客などの関係者に周知しましょう。

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

(2) 実施状況の把握

「5分でできる！情報セキュリティ自社診断」(付録3)を利用して、情報セキュリティ対策が、どれくらい実施できているかを把握します。自社診断は、表4に示す25項目の設問に答えるだけで情報セキュリティ対策の実施状況が把握できるツールです。

具体的な使い方は以下のとおりです。

- ●経営者または情報システム担当や部門長など実施状況が分かる人が「5分でできる！情報セキュリティ自社診断」の診断編に記入します。
- ●事業所が複数ある、部署数が多いなど、一人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- ●実施状況が分からない場合は、各従業員に質問して、回答を総合して記入します。
- ●チェック欄の該当するもの1つに○を付けて、「実施している　4点」「一部実施している　2点」「実施していない　0点」「わからない　－1点」で採点します。
- ●全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「わからない」になっている項目を把握します。

【表４】自社診断のための25項目

No		診断内容
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？

※１　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※２　重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。

(3) 対策の決定と周知

診断結果をもとに、「5分でできる！情報セキュリティ自社診断」の解説編を参考に、実行すべき情報セキュリティ対策を検討します。自社診断には、あまり費用をかけず、効果があると考えられる対策例が示されているので、診断結果に基づき、実施すべき対策を検討します。

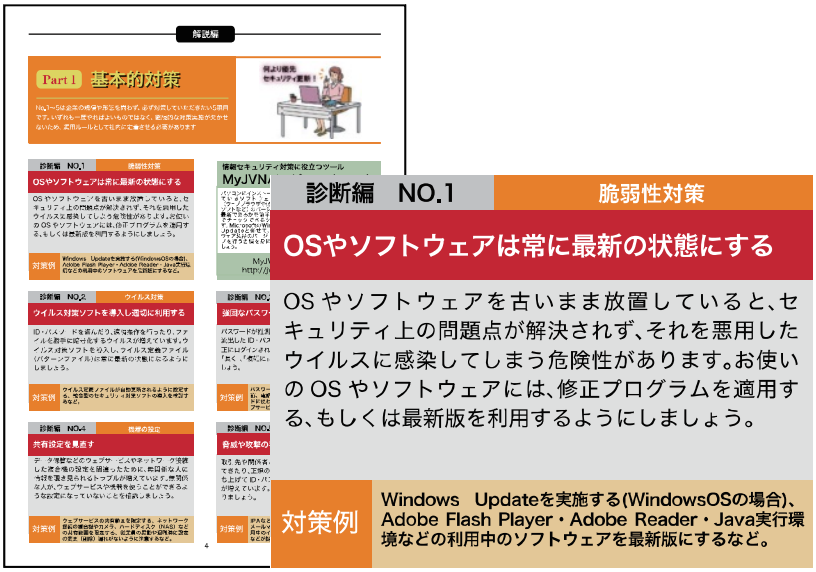
具体的な使い方は以下のとおりです。

●対策の検討と決定は、責任者・担当者と経営者が行います。

●診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討します。

●検討するときには従業員の意見を聞き、職場環境や業務に適した対策を決定します。

「5分でできる！情報セキュリティ自社診断」解説編



対策が決まったら、**「情報セキュリティハンドブック(ひな形)」(付録4)**を利用して、従業員が実行するべき事項を周知します。情報セキュリティハンドブック(ひな形)は、自社診断の対策例と連動したひな形です。決定した対策を具体的に記述して、従業員に配付します。

具体的な使い方は以下のとおりです。

●情報セキュリティハンドブックは、責任者・担当者が作成します。

●ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。

(例)データのバックアップ

編集前(ひな形)

機器名	対象	方法	保管媒体	頻度
○○サーバー	システムファイル ユーザーファイル	Windows バックアップ	外付け HDD	毎週

編集後

機器名	対象	方法	保管媒体	頻度
営業部 ファイルサーバー	売買契約書ファイル	バックアップソフトによる 増分バックアップ	外付け HDD	毎週

●完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、情報セキュリティ対策を周知徹底します。

コラム

「SECURITY ACTION」二つ星へステップアップ！

IT化社会では、情報の取り扱いに関して安心して利用できる、発注できる、取引できる会社であることが求められるようになってきました。しかし、顧客や相手の会社に、自社が情報セキュリティに取り組んでいるかどうかを具体的に示すのは、とても難しいことです。顧客や取引先に情報セキュリティ対策への取り組みを明確に伝え、信頼を獲得するために「二つ星」を宣言してみませんか。

「二つ星」は、「3. 組織的な取り組みを開始する」を実施したことを宣言するものです。

- **「5分でできる！情報セキュリティ自社診断」で自社の状況を把握**
- **「情報セキュリティ基本方針」を定め、外部に公開**

宣言方法や「一つ星」からのステップアップについては公式サイトをご確認ください。

SECURITY ACTION ★★
セキュリティ対策自己宣言

●SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/

4 本格的に取り組む

自社に適した対策を実行して効果をあげるには、まず、自社にどのような情報セキュリティリスク（事故が発生したとき事業へ損害を与える危険性のこと。以下、「リスク」といいます。）があるかを考えます。経営者が懸念する情報セキュリティ上の重大事故やその関連業務などを踏まえ、事業へ大きな損害を与える事故を防ぐための対策を決めて、具体的に記述します。（対策を記述した文書のことを、以下、「規程」といいます。）

(1) 管理体制の構築

①責任分担と連絡体制の整備

P.18（1）情報セキュリティ基本方針の作成と周知にて作成した情報セキュリティ基本方針を具体的に実現するための、情報セキュリティ対策を推進する管理体制を決めます（表５）。情報セキュリティ責任者から部門責任者を通じて従業員への情報の伝達経路を確立し、また情報セキュリティ上の事故などが発生した場合は、情報セキュリティ責任者へ状況が迅速に報告されるような連絡体制を整備することが重要です。すでに個人情報保護管理体制（特定個人情報事務取扱担当者、個人情報苦情申出先）などが決まっている場合は、既存の管理体制との整合をとるようにしましょう。

【表５】情報セキュリティ管理のための役割と責任分担（例）

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

なお、情報セキュリティ組織の担当者がそれぞれの役割を果たすためには、情報セキュリティに関する知識や経験も必要です。知識の習得や経験には時間も必要になるため、中長期の視点で担当者を育成することも考えましょう。

また、小規模な企業などでは、表５の例にとらわれずに、実効的な体制（役割分担）を独自に考えることもあり得るでしょうが、誰か一人に情報セキュリティ対策の全てを任せてしまうような体制は望ましいものではありません。

②緊急時対応体制の整備

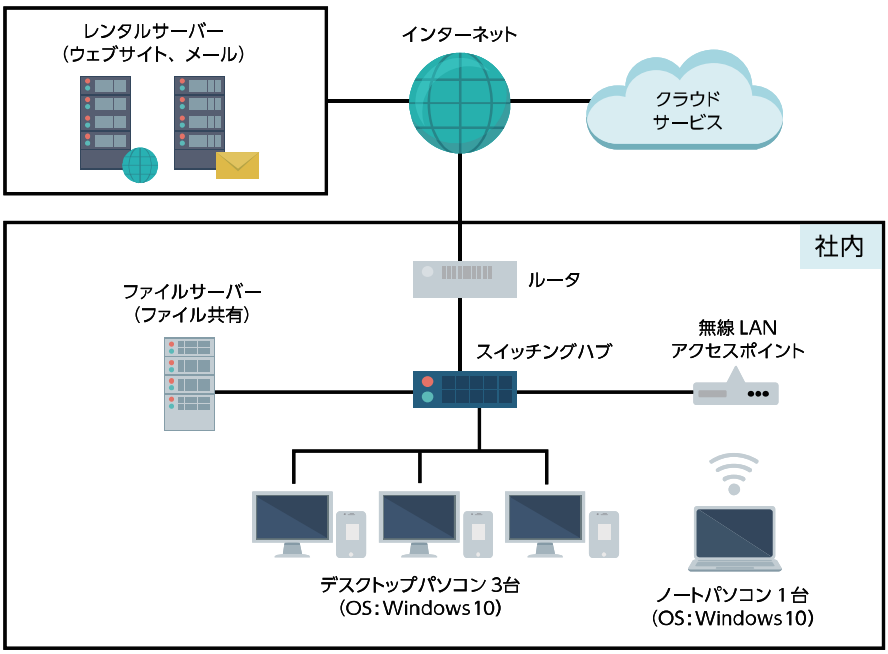
事業や顧客などに大きな影響がある情報セキュリティ事故が発生した場合に、迅速に対応するための体制をあらかじめ決めておきます(表６)。対応を誤ったり、遅れると、被害が拡大したり、復旧がうまくいかずに、取り返しのつかないことになるため、誰が何をするか役割や手順を明確に決めておく必要があります。また、組織内外の緊急連絡先・伝達ルートを整備し、周知しておくことも重要です。加えて、緊急時対応に関する話し合いや訓練などを実施し、実際に決めたとおりに動けるのかを確認するようにしましょう。関係者やIT製品のメーカー、保守ベンダー等への連絡先もまとめておきます。業務システムが使えなくなるような事故においては、メールやwebブラウザも使えなくなる可能性があるため、連絡の代替手段も確認しておきましょう。

【表６】緊急時対応体制の役割と責任(例)

役職名	役割と責任
情報セキュリティ責任者	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者	対応責任者の判断・意思決定に基づき適切な処置を行う。事故の原因を調べて情報セキュリティ責任者に報告する。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告する。

(2) IT利活用方針と情報セキュリティの予算化

企業運営においてITの利活用による生産性の向上や業務の効率化を進めることは重要な課題です。従来はIT機器やソフトウェアを購入して自社内に情報システムを構築することが多かったのですが、現在はレンタルサーバーやクラウドサービスなど外部サービスも増えたため、IT利活用のしかたは多様化しています。それに伴いリスクも多様化しているため、自社で利用している情報システムについて、例えば台帳を作成したり図式化したりするなどして把握したうえで、対策を検討するとともに、予算を確保する必要があります。



(3) 情報セキュリティ規程の作成

企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ITの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。そこでここでは、効率的に自社に適した規程を作成する方法を解説します。

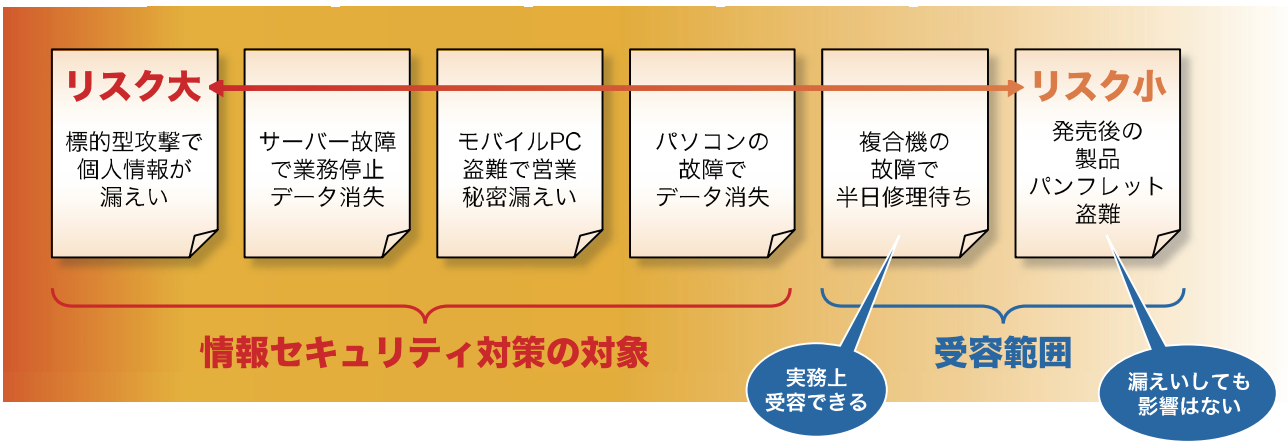
①対応すべきリスクの特定

経営者が懸念する避けるべき情報セキュリティの重大事故などを踏まえて、何が起こらないようにするべきかを考えます。この時、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

●関連する業務や情報に係る外部状況(法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など)
●内部状況(経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など)

②対策の決定

全てのリスクに対応しようとすると費用が多額になったり、仕事が非効率になることがあります。そこで、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものを優先して対策を実施し、事故が起きる可能性が小さいか、発生しても被害が軽微であるなど、リスクが小さなものについては、現状のままにするなど、合理的に対応します。



③規程の作成

②で決定した対策を文書化した規程を作成します。決定した対策を一から文書化するのは経験がないと難しいため、**「情報セキュリティ関連規程（サンプル）」（付録５）**を参考に、自社に適した規程にするために修正を加えます（表７）。

サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成します。なお、サンプルに明記されていなくても必要な対策や有効な対策があれば、追記を行ってください。

【表７】情報セキュリティ関連規程（サンプル）の概要

	名　称	概　要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。

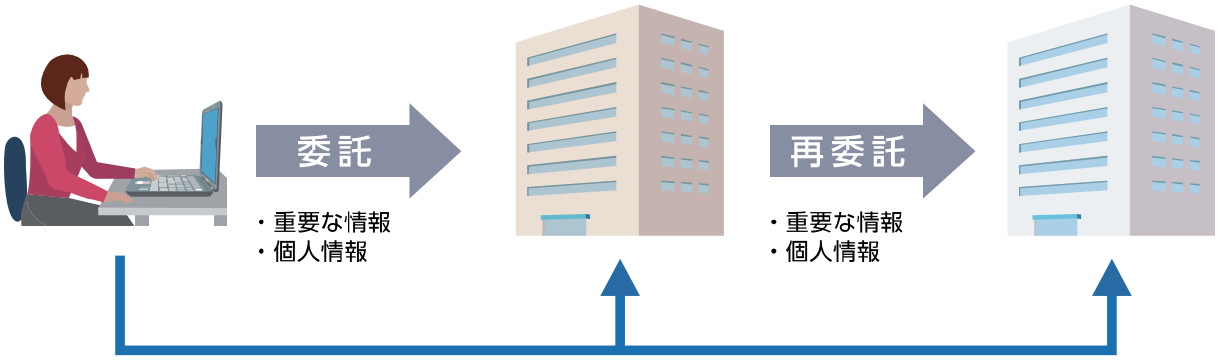
(4) 委託時の対策

社内業務の一部または全部を外部に委託したり、レンタルサーバーやクラウドサービスなどの外部サービスを利用することが一般的になっています。重要な情報を渡したり、処理を依頼する場合には、委託先にも情報セキュリティ対策を実施してもらう必要があります。

直接指示することが難しい外部の組織に、対策を実施してもらうには、取引条件のひとつとして契約書や覚書などに具体的な対策を明記します。個別に契約や覚書を交わすことができない場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確認したうえで選定します。

また、個人情報保護法では、個人データ[7]の取り扱いを委託する場合は、委託先にも情報セキュリティ対策を実施してもらうように監督することが義務付けられています。委託先の状況を把握し、対策が確実に実施されるように委託元が責任をもつ必要があります。

委託先の対策不足で事故が起きた場合には、委託元は管理責任を問われ、委託先は委託元の信頼を失います。重要な情報や個人情報などセキュリティ事故の影響が大きい情報の授受が行われる場合には、委託元は委託先にセキュリティ対策についての要望や期待をしっかりと伝え、受託する側はそれをきちんと理解し、実行する必要があります。



これらを踏まえ、取り扱う情報の種類、委託する業務に適した情報セキュリティ対策を委託先にも実施してもらいます。機密情報や個人情報を取り扱う場合は、「情報セキュリティ関連規程(サンプル)」(付録5)の「業務委託契約に係る機密保持条項」を参考にして、委託先と契約したり、委託先を選定してください。さらに、情報セキュリティ対策が継続して実施されているか、新たな対策が必要になったときに対応しているかなどを随時確認して、委託先の情報セキュリティ対策が維持されているか、責任をもって管理します。

7 ▲個人情報保護法では「個人情報」、「個人データ」、「保有個人データ」、「要配慮個人情報」、「匿名加工情報」等の語を使い分けており、個人情報取扱事業者等に課される義務はそれぞれ異なるので、注意を要します。

コラム

委託と受託

委託とは他者に業務を行ってもらうことです。外注、委任、準委任、アウトソーシングなどということもあり、受託とは他者の業務を引き受けることで、請負ということもあります。

どのような会社でも事業を行ううえで、全ての業務を自社で行うことは難しいため、委託している業務があり、委託とそれを引き受ける受託とで成り立っています。また、業務を委託するときには、委託元と委託先との間で情報の授受が発生します。

例えば、以下のような皆さんの身近な業務で、情報を授受していませんか。

●税理士に帳簿や決算書の作成を依頼　：売上伝票、出金伝票
●外部の工場に部品の製造を依頼　　：設計図
●システム開発会社にECサイトの運用を依頼：住所、氏名など顧客の個人情報

このように重要な情報や個人情報を渡す場合に、委託先が対策を怠っていれば、漏えいや改ざんなどの事故が起きやすくなります。

業務を受託する場合においては、発注元が求めるセキュリティ対策を実施できることを示す必要があります。自己点検の結果や、SECURITY ACTIONのロゴマークを提示したり、具体的な規程の内容や、システム上の対策例を閲覧してもらうことで、相手の信頼を得ましょう。

(5) 点検と改善

情報セキュリティの点検とは、計画した情報セキュリティ対策が、本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、を確認することです。点検の基準には以下を用いることができます。

その１)「情報セキュリティ５か条」や「５分でできる！情報セキュリティ自社診断」に基づく点検

点検基準例

☑**「情報セキュリティ５か条」No.1の対策例を基準にする。**
パソコンのWindowsUpdateが「更新プログラムを自動的にインストールする」に設定されていて、更新日が直近の日付であるか

☑**「５分でできる！情報セキュリティ自社診断」No.20の対策例を基準にする。**
従業員に情報セキュリティ事故のニュースを周知したり、情報セキュリティ啓発サイトの新着情報を配信するなどしているか

その２)策定した情報セキュリティ対策に関するルール・規程に基づく点検

点検基準例

☑**ウイルス感染時の初期対応のルールを基準にする。**
社内規程の中で、ウイルス感染時の対応に関する記述を理解しているか
(「情報セキュリティ関連規程(サンプル)」No.10「情報セキュリティインシデント対応ならびに事業継続管理」の該当項目を参照)

点検には、以下の方法があります。

- ●質問(インタビュー)　:従業員や委託先の管理者などに直接質問して回答してもらう
- ●閲覧(レビュー)　:関連する文書や記録、パソコンの設定画面など対策を実行した証拠となるものを確認する
- ●観察(視察)　:点検の対象となる職場に出向き、従業員が規程や標準規格などに従った行動をしていることを確認する
- ●技術診断　:専用ソフトウェアなどを使ってコンピュータやネットワークのセキュリティ対策が実行されているかを確認する
- ●チェックリスト　:チェックリストや質問書を配付して回答してもらう

点検の結果を経営者に報告し、経営者の意図するセキュリティ対策が実現できているかの確認と評価をすることが重要です。経営者の評価を得ることで、場合によってはリスクの特定に戻って対策の見直しをするなどにより、取り組みの精度を高めていくことになります。

なお、営業秘密や個人情報等の、特に十分な対策が必要な場合には、第三者による情報セキュリティ監査[8]を行うことも検討します。

8▲一般に、点検は点検対象業務に従事している関係者自身が実施するのに対し、監査は監査対象業務に従事していない、独立した監査担当者によって実施されるため、より客観的な確認を行う必要がある場合には監査が適しています。

コラム

情報セキュリティ点検の実施例

「情報セキュリティ５か条」に取り組んでSECURITY ACTION一つ星を自己宣言している会社が、「情報セキュリティ５か条」を基準にして点検するときの実施例です。

①No.1「OSやソフトウェアは常に最新の状態にしよう！」について社員の一人に、質問と閲覧で点検します。


「情報セキュリティ５か条」では OS やソフトウェアは常に最新の状態にすることになっていますが、持出し用のノートパソコンの OS やソフトウェアは最新の状態でしょうか？」


「ノートパソコンをしばらく使っていないので、分かりません。」


「では、Windows Update の更新プログラムのインストール履歴を見せてください。」


「（ノートパソコンの画面に更新プログラムのインストール履歴を表示）」


「画面を見ると最後のインストール履歴が２か月前になっていますが、理由はわかりますか？」


「Windows Update は自動更新に設定していますが、このノートパソコンは社外に出かけるときだけに使うので、普段はネットワークに接続していません。それで更新されていないのだと思います。明日、お客様の事務所に伺い、このノートパソコンをお客様の LAN につないでメールを使いますので、それが終わったら更新しようと思います。」

②ノートパソコンを持ち出すことがある他の社員に、質問やパソコンの画面を見せてもらい、その回答や観察の結果から総合的に判定します。

この例では、「情報セキュリティ５か条」の「OSやソフトは常に最新の状態にしよう！」を実行できていないパソコンがあることを発見しました。その状態でお客様のLANに接続する予定であったことから、影響が社外におよぶ可能性があり、リスクが大きいと言えます。このようにリスクが大きいと考えられる場合は、すぐに是正するよう助言します。

点検というと難しく思えるかもしれませんが、スポーツの審判のように、ルールを基準とし、選手が基準を満たしているか判定することと同じです。客観的に評価、判定することで、気付かなかった不備が明確になりますので、情報セキュリティのレベルアップにはとても役に立ちます。